DOD Medium Assurance Public Key Infrastructure (PKI)

Adam K. Britt, D25

02 December 1998

(703) 681-7964

DSN 761-7964

britta@ncr.disa.mil

Topics

- **Program Goals**
- **PKI Assurance Levels**
- **PKI Functionality**
- **PKI Operational Responsibilities**
- **PKI Architecture**
- **PKI Programmatics**
- **Challenges**
- **Summary**

Program Goals

- **Encompass all assurance levels**
- **Minimize costs through common infrastructure and services:**
  - **Minimize cards/token per individual**
  - **Minimize registration requirements**
  - **Single Directory service**
  - **Interoperability internal/external to DOD**
  - **Standards-based to facilitate commercial products (i.e. FIPS 140)**

PKI ASSURANCE LEVELS

Proposed Assurance Levels Implementation Examples

POLICY	BASIC	MEDIUM	HIGH
User Authentication	Some type of check performed (may rely on personal knowledge)	In person with official ID OR personal knowledge	In person with 2 official IDs, 1 picture ID
Key Pair Generation	Performed in SW	Performed in SW or HW	Performed in HW
User Private Key Protection	FIPS 140-1 Level 1 Cryptomodule (No Trust in OS)	FIPS 140-1 Level 1 (Used with self-protecting OS)	FIPS 140-1 Level 2 (Used with self-protecting OS)
CA Private Key Protection	FIPS 140-1 Level 2	FIPS 140-1 Level 2 w/Level 3 Key Mgmt	FIPS 140-1 Level 2 w/Level 3 Key Mgmt and roles/services

PKI FUNCTIONALITY

"THE" DIGITAL ID FOR DOD PERSONN

"THE" DOD WHITE PAGES DIRECTORY

PKI Functionality

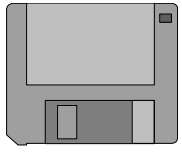
"THE" DIGITAL ID FOR DOD PERSONN

- **All personnel would have medium assurance certificate**
- **Certificate would be used by any application to identify/authenticate, support access control, digitally sign, etc.**
- **Permissions embedded in application, not certificate**
- **Some portion of users would also have high assurance certificate (FORTEZZA).**

PKI Functionality (cont.)
User Tokens

Basic and Medium Assurance:

Today



Floppy
FIPS 140-1 Level 1

Future

ISO Smartcard
FIPS 140-1 Level 1

High Assu

FIPS 140-1 Level 2

PKI Functionality (cont.)

"THE" DOD WHITE PAGES DIRECTOR

- **User will see one integrated Directory Service**
- **Medium Assurance PKI Directory will store individual information**
- **High Assurance PKI Directory for DOD organizational, GENSER PLA, and SI PLA requirements**

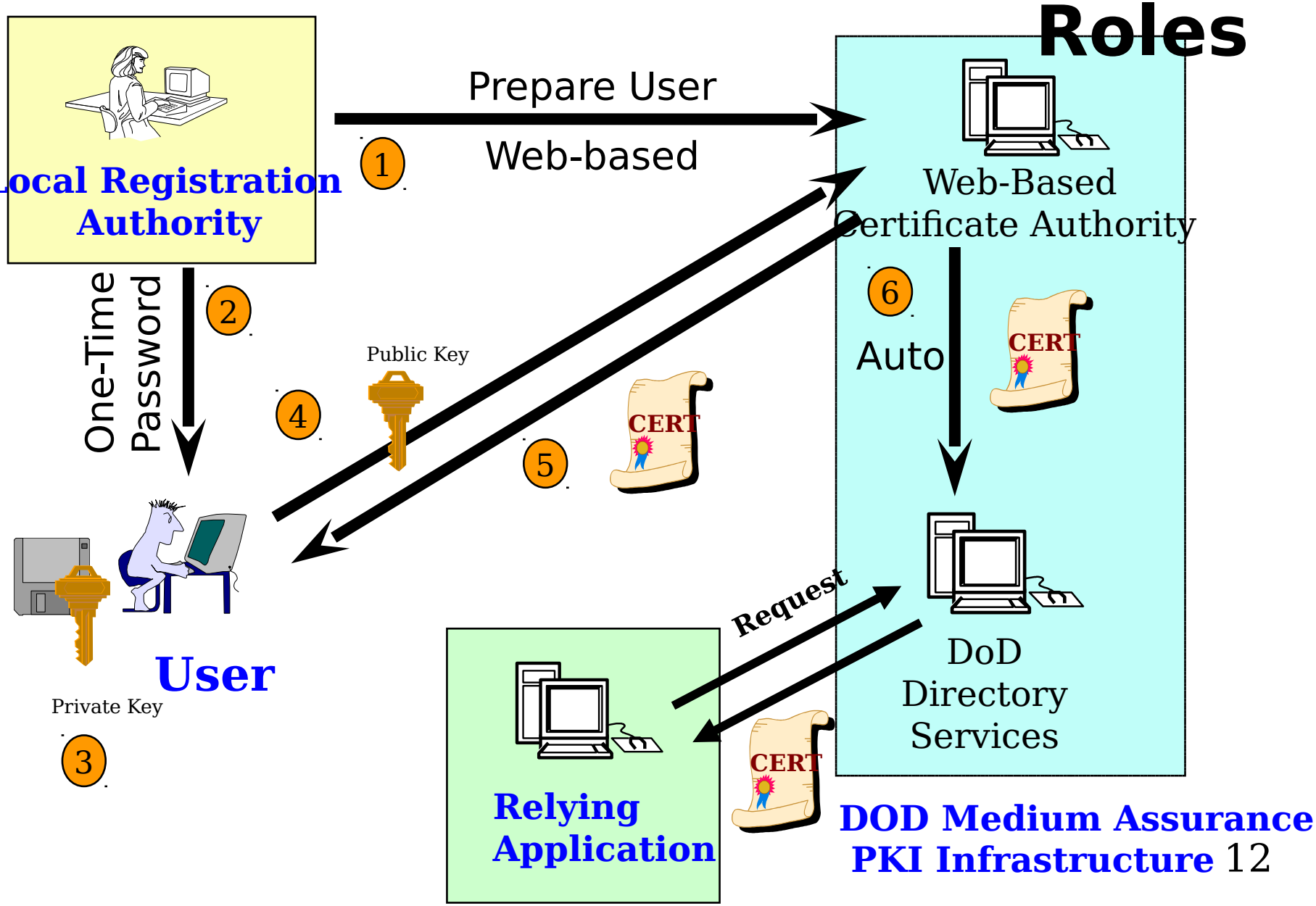
  Fulfill ACP 133 Requirements

PKI OPERATIONAL RESPONSIBILITIES

PKI Operational Responsibilities

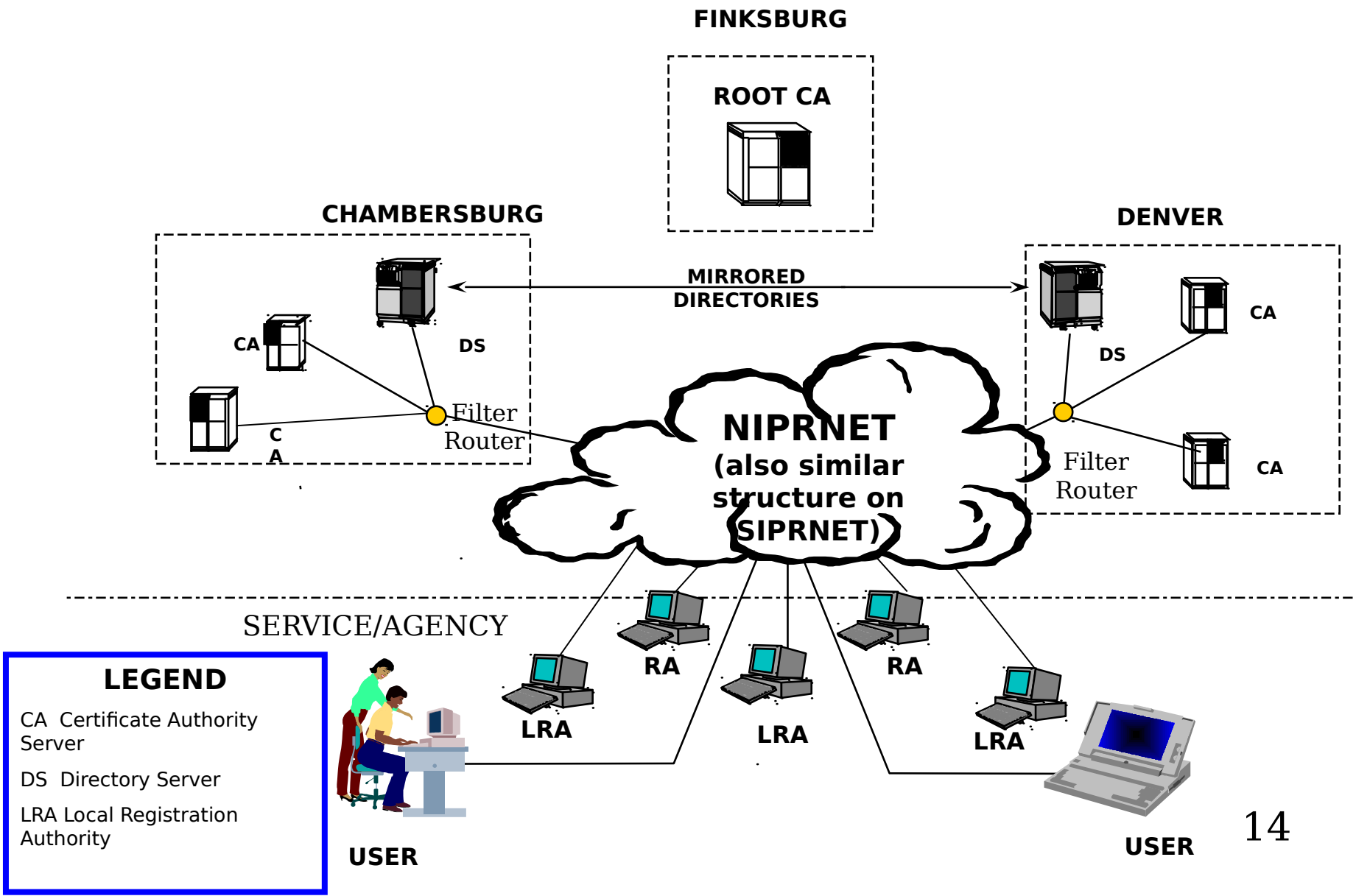
- Certificate generation, posting, revocation, archiving
  - DISA, NSA
- User registration
  - Services and Agencies
- Data recovery capability
  - Initially, local organizations retain keys
  - With next PKI, infrastructure retains keys
- Application mod / development
  - COTS developers
  - DOD Program Office or organization

Medium Assurance PKI Roles



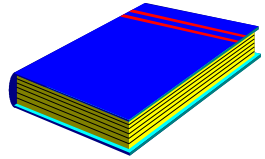
PKI ARCHITECTURE

Near-Term Medium Assurance DOD PKI Architecture



DOD PKI Documentation

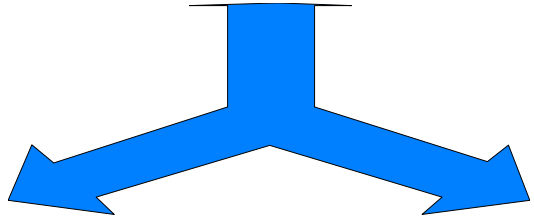
DOD PKI
CERTIFICATE POLICY (CP)



Draft
Version 3
25 Nov 97*

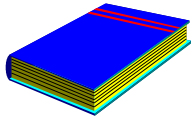
MEDIUM ASSURANCE

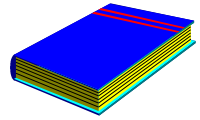
HIGH ASSURANCE



CERTIFICATION PRACTICE STATEMENT (CPS)

Draft
Version 1
May 98

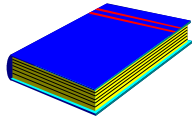


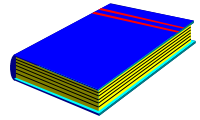


ISSP CPS
5 May 97

CONCEPT OF OPERATIONS

DII PKI
CONOPS
3rd Draft,
24 Oct 97

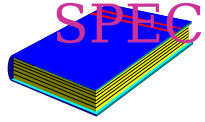


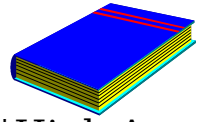


MISSI SMI
CONOPS
8 Oct 96

INTERFACE SPECIFICATIONS

Generic in
draft;
11 May 98





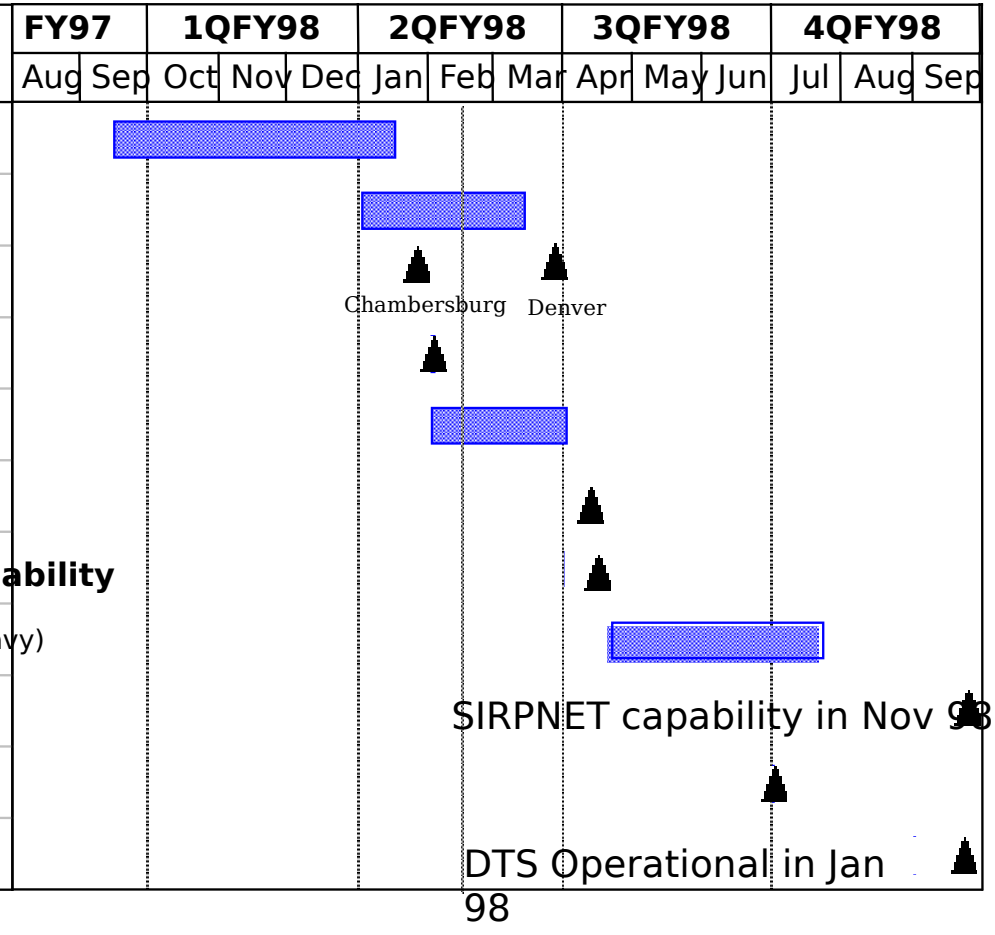
SDN 908
(MMP)

*High Assurance currently covered by

PKI PROGRAMMATICS

DOD PKI Schedule

ID	Task Name
1	PKI System Development
2	PKI Test and Certification
3	Install Infrastructure at DMCs
4	**PKI Available: Testing**
5	Support Test Users
6	Establish Root CA
7	**PKI Operational: Initial Availability**
8	NIPRNET Limited Users (EDA, DSS, Navy)
9	SIPRNET Limited Availability
10	**PKI Operational**
11	DTS IOC



PKI Pilot Users

- **DISA**
  - 20 Users (April 98)
  - Network access control
- **Joint Electronic Commerce Program Office**
  - 8000 Users (April 98)
  - Network Access Control
- **Defense Security Service**
  - 300 Users (beginning April 98)
  - Secure e-mail
- **Joint Engineering Data Management Information and Control System (JEDMICS)**
  - 26,000 Users (Aug 98)
  - Data Access Control
- **DOD Inspector General**
  - 35 Users initially, potentially several hundred (Apr/May 98)
  - Secure e-mail
- **Defense Travel System**
  - 250,000+ Users (by 4QFY99)
  - Claim signatures

DOD PKI Working Group

Chair: DISA D25

Service/Agency Representatives:

- **Army:** COL Michael Brown, ODISC4, (703) 697-1474
  Gary Robison, ODISC4, (703) 614-5705
- **Navy:** Bob Buchanan, DCMS (202) 764-0003
  CDR Chris Perry, CNO N64 (703) 601-1253
- **Air Force:** Roland Drumm, AFCA (618) 256-2498
  Neil Knowles, AFCIC (703) 697-2108
- **Marine Corps:** Gilda McKinnon, HQMC, (703) 614-3591
- **Joint Staff :** CDR Nick Harris, J6K, (703) 614-5990
- **DLA:** Stacy Hopkins, DLA/AQAC, (703) 767-3117
- **DFAS:** Ethel Matthews, DFAS HQS, (703) 607-3971
- **DIA:** Robert Cole, DIA, (202) 231-2182
  Gary Strohm, DIA, (202) 231-2018
- **NSA:** Don Heckman, X35, (410) 859-4537
- **DISA:** Becky Harris, DISA D25, (703) 681-7973

Challenges

- **Non-interoperability of current commercial products**
  - **Standards too broad-based**
  - **Need profile to be more specific**
- **Current market products are immature**
- **Desire for PKI services now**
  - **Deployment of non-interoperable solutions**
- **Processes and procedures are paramount**
  - **Some developed**
  - **Others TBD**

Summary

Single DOD-wide PKI will:

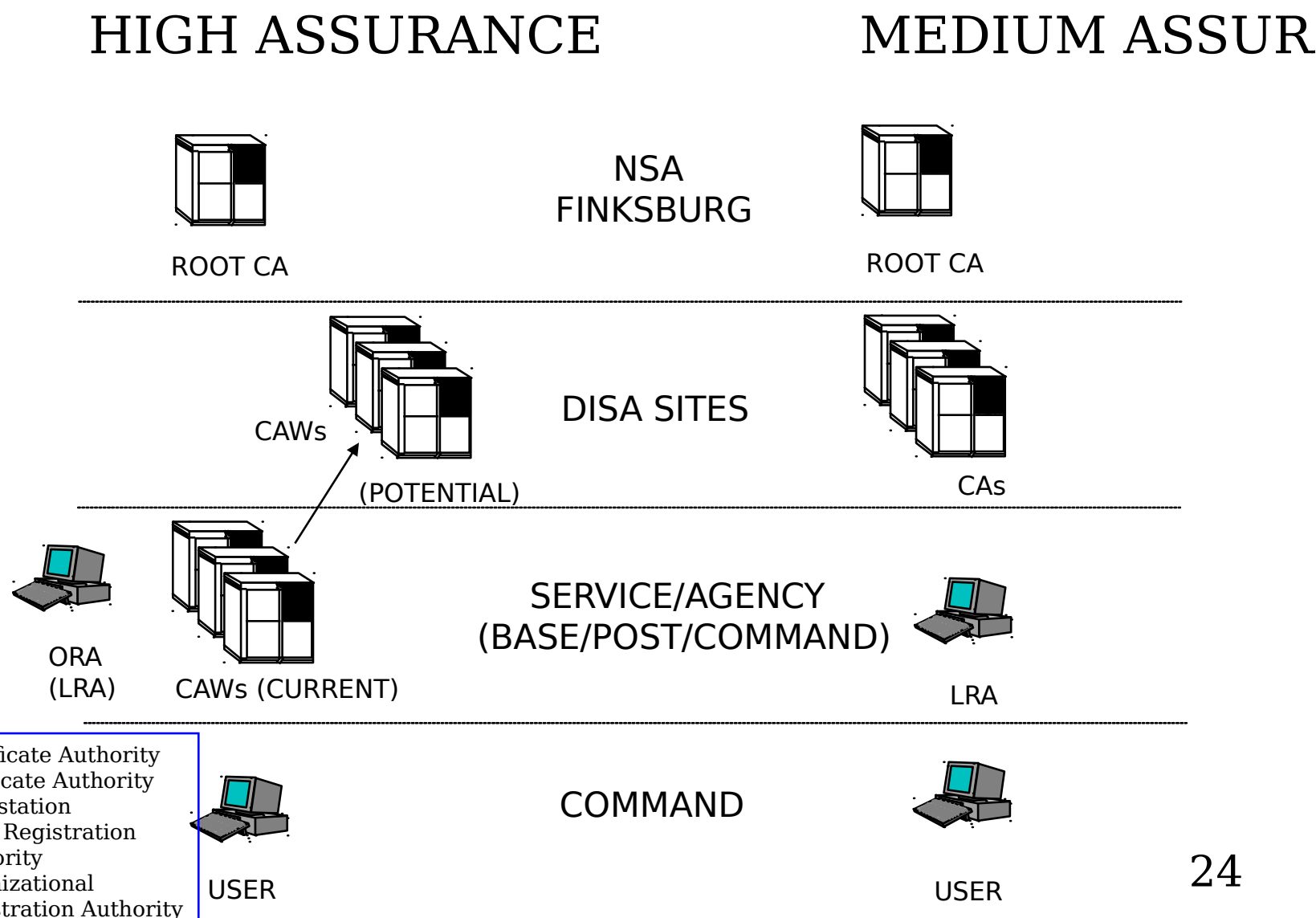
- **Incorporate all assurance levels**
- **Minimize costs of implementation**
- **Provide single Directory Service**
- **Provide interoperability both within and without DOD**

BACKUPS

Certificate Generation, Posting, Revocation, Archiving

- All medium assurance CAs would be run by DISA
- Currently, high assurance CAWs run by services
- With upcoming remote CAW capability, high assurance CAWs could be centralized with medium assurance CAs
  - Reduce service manning requirements
  - Still allow service control over registration; FORTEZZA generation

CA/LRA Placement



User Registration

- **For medium assurance users:**
  - **All DOD users would need to be registered**
  - **Potentially valid for extended period of time**
  - **Certificate information not tied to job**
  - **Service/Agency personnel centers could provide central locations; capitalize on existing ID processes**
- **For high assurance users:**
  - **Registration requirement based on current job/organization.**
  - **Command/organization would provide registration (ORA)**

Funding Strategy

- **DISA to procure/establish infrastructure**
  - **Certificate Authorities**
  - **Directory Servers**
  - **User Registration Software**
  - **Archives as appropriate**
  - **Help Desk**
- **Services to provide registration-related items:**
  - **Registration Authority (RA), Local Registration Authority (LRA) and user workstations (do not need to be dedicated)**
  - **Smartcard readers for RA and LRA Workstations**
  - **User tokens/readers (floppies initially)**
- **Operations & Maintenance**
  - **PKI will be integral part of DII, funding strategy TBD**

Why Netscape

- **Only commercial product currently certified as FIPS 140-1 compliant**
- **Netscape shares DISA vision of**
  - **Open Standards**
  - **Commercial Interoperability**
  - **Data Recovery**
- **DISA Enterprise License w/Netscape provides**
  - **DOD leverage in product features**
  - **Economies in fielding**
  - **Timeliness in meeting DTS fielding schedule**